Security Policy #3

Security Incident Procedures

Purpose of Policy

The purpose of the policy is to develop the response to and reporting of security incidents, including the identification of and response to suspected or known security incidents, the mitigation of the harmful effects of known security incidents, to the extent possible, and the documentation of security incidents and their outcomes.

It should be noted that breach definitions, remediation steps and breach notification steps vary between various federal regulations such as the Health Insurance Portability and Accountability Act (HIPAA), The Gramm-Leach-Bliley Act (GLB Act or GLBA) and other federal regulations. In addition, most state regulated breach laws vary between individual states. In is highly recommended to consult with breach experts or legal counsel to determine The Company's responsibilities.

Definitions

Breach

Breach means the acquisition, access, use, or disclosure of personally identifiable information (PII) or sensitive company data such as email, employee information, confidential information, etc. which compromises the security or privacy of the PII or sensitive company data.

Unsecured PII

Unsecured PII means PII that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology such as encryption. The definition of unsecured PII varies between different federal and state regulations.

Reporting and Response

1. The Company will ensure that all incidents, threats, or violations that affect or may affect the privacy, confidentiality, integrity, or availability of PII and sensitive company data will be reported and responded to.

2. The Company shall have a Security Incident Response Team (SIRT) charged with the responsibility of identifying, evaluating and responding to security incidents. The Privacy Security Officer shall oversee the activities of the SIRT.

    a. The SIRT will be responsible for investigating all known or suspected privacy and security incidents.

    b. The SIRT will document a procedure for all employees to follow to report privacy and security incidents. See **Appendix A – Security Incident Response Log or the Security Incidents Module in the Security Portal.**

    c. The Company will ensure that all employees receive training on how to identify and report security incidents.

    d. All employees must follow the documented procedure to report security incidents. In addition, employees must report all known or suspected security incidents.

    e. All employees must assist the SIRT with any security incident investigations.

Breach Determination

The Security Incident Response Team (SIRT) will investigate all reported and suspected security breaches. The SIRT will refer to federal or state regulations to help with breach determination. Breach determination varies between federal regulations such as HIPAA and GLBA. In addition, breach determination varies significantly between state regulations (for example, what may be considered a breach in one state may not be a breach in another state).

Breach Notification

If the SIRT determines that a breach of unsecured PII has occurred, breach notification of affected individuals may be required. The SIRT will refer to federal or state regulations to help with breach notification requirements. Breach notification requirements varies between federal regulations such as HIPAA and GLBA. In addition, breach notification requirements vary significantly between state regulations (for example, one state may have breach notification requirements that varies significantly from breach notification requirements in another state).

Key elements of a breach notification include:

I. Date of discovery

Usually, a breach will be treated as discovered as of the first day the breach is known or by exercising reasonable diligence would have been known.

II. Timeliness of notification

The Company will provide the required notifications without unreasonable delay after discovery of a breach. The amount of time The Company has to notify affected individuals varies between federal and state regulations.

III. Content of notification

If required, a notification will be provided to each individual affected by the discovered breach. The notification should include the following:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
- A description of the types of unsecured PII that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number or other types of information were involved).
- Any steps individuals should take to protect themselves from potential harm resulting from the breach.
- A brief description of what The Company is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which should include a telephone number, an e-mail address, Web site, or postal address.
- The notification should be written in plain language.

IV. Methods of notification

The following methods are usually used to notify individuals affected by the discovered breach:

i. Written notice

Written notification by first-class mail to the individual at the last known address of the individual or, via e-mail if the individual agrees to e-mail notice. The notification may be provided in one or more mailings as information is available.

If the individual is deceased notifications are usually sent to next of kin or personal representative

ii. Substitute notice

If contact information is out of date and written notification cannot be made, a substitute notification may be used.

- A substitute notification usually in the form of either a conspicuous posting on The Company's home page of its Web site, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. The notice should include a contact phone number.

V. Notification to media

In addition to notifying individuals of a known breach, a notification to the media may be required as well.

VI. Notification to federal or state regulatory agencies

The Company may need to report breaches of unsecured information to federal or state regulatory agencies.

VII. Notification by Third Party Service Providers

Third Party Service Provider responsible for a breach of The Company's PII or sensitive company data should be required to notify The Company within a pre-determined reasonable timeframe. The timeframe should be defined in a Service Provider Agreement.

Third Party Service Provider breaches may result in The Company having to notify The Company's affected individuals (such as customers, employees, etc.).

Appendix A – Security Incident Response Log

Incident Identification Information	
Name:	
Phone:	
Email:	
Date/Time Detected:	
System / Application Affected:	
Incident Summary	
Type of Incident Detected: (Denial of Service, Malicious Code, Unauthorized Access, Unauthorized Use / Disclosure, Unplanned System Downtime, Other)	
Description of Incident:	
Names of Others Involved:	
Incident Notification	
How Was This Notified? (Security Office, IT Personnel, Human Resources, Email, Other)	Email: 3p-security@amazon.com
Response Actions **Include Start and Stop times**	
Identification Measures (Incident Verified, Accessed, Options Evaluated):	
Containment Measures:	
Evidence Collected (Systems Logs, etc.):	